REMARKS

Claims 1-30 are currently pending in the subject application and are presently under consideration. Claims 1, 5, 11, 15, 21, and 25 have been amended as shown on pp. 2-8 of the Reply.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-30 Under 35 U.S.C. §103(a)

Claims 1-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Nessett *et al.* (U.S. 6,766,453) in view of Berman *et al.* (U.S. 2003/0221126) and Dujari *et al.* (U.S. 7,191,467). Withdrawal of this rejection is requested for at least the following reasons. The cited references, either alone or in combination, do not disclose or suggest all features recited in the subject claims as amended. "To reject claims in an application under §103 . . . the prior art reference (or references when combined) must teach or suggest all the claim limitations." *See* MPEP §706.02(j); s*ee In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Independent claim 1 (and its corresponding dependent claims) recites: *A method for registering a first device with a second device, comprising the steps of:* ***initiating communication between the first device and the second device over a first communication channel using a first communication method by engaging a trigger at the first device and detecting at the second device that the trigger at the first device has been engaged;*** *generating a first secret known to the first device and a second secret known to the second device using communications between the first device and the second device over the first communication channel using the first communication method; from the first device, producing first information derived from the first secret; from the second device, producing second information derived from the second secret; using a communication channel other than the first communication channel and a communication method other than the first communication method, comparing the first information and the second information in a manner sufficient to assure a third party that the first secret and the second secret are the same; and enabling the first and second device to use the first and second secrets upon the third party being assured that the first*

secret and the second secret are the same. The subject amendments are supported by the specification. For example, the specification describes that a registration process between two network devices can be initiated by one of the network devices upon activation of a trigger, such as a button or a switch, on the network device. (*See* p. 7, ll. 21-23; p. 20, ll. 20-23).

Nessett *et al.* relates to techniques for performing an authenticated Diffie-Hellman key agreement protocol over a network where the communicating parties, such as a client device and a wireless network access point, share a secret key with a third party. (*See* col. 2, ll. 40-47). Under the protocol described by Nessett *et al.*, a wireless client system and a network access point transmit a secret key to a third party RADIUS server. (*See* col. 2, ll. 52-57; col. 7, l. 63 – col. 8, l. 7). Once both secret keys have been transmitted, the client system can initiate registration by generating a first registration message and communicating the message to the network access point. (*See* col. 2, ll. 58-67; col. 8, ll. 8-39). In turn, the network access point generates a second registration message and transmits the first and second messages to the RADIUS server for authentication. (*See* col. 3, ll. 1-11; col. 8, l. 40 – col. 9, l. 5). However, independent claim 1 recites ***initiating communication between the first device and the second device over a first communication channel using a first communication method by engaging a trigger at the first device and detecting at the second device that the trigger at the first device has been engaged***. Nessett *et al.* does not disclose or suggest such novel features. Specifically, prior to registration, Nessett *et al.* discloses that a network device and a network access point provide secret keys to a RADIUS server. Nessett *et al.* then discloses that registration between the network device and network access point begins by generating registration information at the network device. However, Nessett *et al.* is silent regarding how the network device and/or the network access point initiate the communication of secret keys to the RADIUS server. Further, after the network device and network access point transfer secret keys to the RADIUS server, Nessett *et al.* is additionally silent as to how the registration process between the device and the access point is initiated. Thus, Nessett *et al.* does not disclose or suggest *initiation of a registration between a first network device and a second network device by engaging a trigger at the first network device* as recited by independent claim 1.

Similarly, Dujari *et al.* does not overcome the noted deficiencies of Nessett *et al.* Dujari *et al.* generally relates to techniques for providing extended functionality for Internet browsers in order to facilitate authentication between an Internet client and a server *via* a third party authentication service. (*See* abstract; col. 6, ll. 46-65). As generally described by Dujari *et al.*, a client and a server communicate *via* the Internet using HTTP. (*See* col. 6, ll. 29-31). A server can then request third-party authentication for a client with which the server is communicating by sending a HTTP authentication challenge to the client. (*See* col. 2, ll. 31-47). Upon receiving this authentication challenge, the client then engages in third-party authentication with a login server. Thus, Dujari *et al.* discloses that authentication is performed by a server by issuing a challenge to the client. Like Nessett *et al.*, Dujari *et al.* therefore differs from the features recited by independent claim 1, wherein registration between network devices is initiated by a network device upon engagement of a physical trigger at that network device.

At Pages 2-3 of the Office Action, the Examiner additionally relies on Berman *et al.* to overcome the deficiencies of Nessett *et al.* and Dujari *et al.* Berman *et al.* generally relates to techniques for mutual authentication between a client and a server. (*See* abstract, paragraph 0010). To begin authentication, a server provides a client with which the server will be authenticated with an object reference that indicates an authentication method used by the server. (*See* paragraph 0045). A secure connection, such as a connection based on SSL, is then established between the client and the server, over which the client sends authentication information, such as a user name and password, to the server. (*See* paragraph 0045, 0062). This information can then be provided to a third party authentication server, such as a DCE security server or a Kerberos server, to authenticate the client with the server. (*See* paragraph 0062).

The Examiner asserts at Page 3 of the Office Action that Berman *et al.* teaches using a communication channel other than the first communication channel and a communication method other than the first communication method, comparing the first information and the second information in a manner sufficient to assure a third party that the first secret and the second secret are the same. However, like Nessett *et al.* and Dujari *et al.*, Berman *et al.* is silent as to ***initiating communication between the first device and the second device over a first communication channel using a first***

communication method by engaging a trigger at the first device and detecting at the second device that the trigger at the first device has been engaged as recited by independent claim 1. Rather, as noted above, the authentication process disclosed by Berman *et al.* begins when the server provides a client to be authenticated with the server an object reference indicating an authentication method used by the server.

Likewise, independent claims 5, 11, 15, 21, and 25 have been amended to recite similar features to those recited by independent claim 1. Thus, Nessett *et al.*, Berman *et al.*, and Dujari *et al.*, either separately or in combination, do not teach or suggest all features of independent claims 5, 11, 15, 21, and 25 for the reasons stated above regarding independent claim 1. Accordingly, Applicant's representative respectfully requests that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP1996US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicant's undersigned representative at the telephone number below.

Respectfully submitted,

Amin, Turocy & Calvin, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

Amin, Turocy & Calvin, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731